

利点

業界最高レベルの検出精度

Cloudmark ActiveFilter では、数秒から数分前に配信されたばかりのスパム・メッセージの検出を可能にすることで、業界で最も優れた Cloudmark Authority® の検出精度をさらに高めています。

再スキャンが不要

Cloudmark ActiveFilter では、メール・ストア内にあるメッセージのうち、分類が変更されたものに対してのみ処理を実行する仕組みになっており、以前に配信されたメッセージを再スキャンする必要がありません。

パフォーマンスへの影響を

最小限に低減

Cloudmark Authority ソリューションと同様、ActiveFilter はシステム・リソースにほとんど影響を及ぼしません。スパム・メッセージのメッセージ ID を調べるだけで済み、数テラバイトから数ペタバイトの電子メールを再スキャンする必要がないからです。

最小限のストレージ要件

Cloudmark ActiveFilter を導入したキャリアの大半は、オンライン・ストレージの必要量を 20% 削減することに成功しています。

キャリアグレードの拡張性

リソース効率のよい ActiveFilter は、最大規模のキャリアの実装環境にも対応可能です。

高度なユーザ・エクスペリエンスを 実現

Cloudmark ActiveFilter を導入すれば、ユーザがスパムやフィッシング攻撃にさらされる危険性を大幅に減らし、顧客満足度の向上と加入者解約率の低減を図ることができます。

メール・ストアを効率的にクリーンアップし、フィルタリング精度の向上を実現

メッセージング・セキュリティの分野では、攻撃者とメッセージング・セキュリティ・ソリューションのプロバイダとの攻防が長く続いてきました。たとえば、ネットワーク侵入防御を突破してユーザの受信トレイにスパムを配信しようとする攻撃者の多くは、スパム防御機能によって検出およびブロックされないうちに、内容を絶えず更新して不正メッセージを配信しています。こうした攻撃者の行為により、スパムの総量が増え、現在では電子メール・トラフィックの 95% 以上をスパムが占めるまでになっています。

スパム送信者が不正メッセージを配信する際には、大規模かつ強力なボットネットなど、きわめて高度な技術を使用します。現在では、世界中のコンピュータの 15% がボットネットに感染しており、これらのコンピュータから全スパムの 90% 以上が配信されています。スパム送信者はボットネットを利用し、内容が常に異なる数百万通のメッセージを 1 分足らずでサービス・プロバイダ・ネットワークから送信しますが、こうした攻撃は検出が難しく、ボリューム・ベースのスパム・フィルタをすり抜けてしまいます。強力なボットネットを構成する 100 万台の各ボット感染 PC が、わずかなメッセージを送信するだけで大規模なスパム攻撃を仕掛けることができるからです。しかも、巧妙に感染する各ボットは、自身がブラックリストに登録されているかどうかを認識できる機能を備えており、特定のサービス・プロバイダ・ネットワークにスパムを引き続き配信できるホストを見つけ出してスパムを送りつけます。

サービス・プロバイダは、こうした攻撃を確実にブロックしなければなりません。最も効果的なフィルタリングおよびスパム対策ポリシーを採用しても、わずかなスパムがすり抜けてメール・ストアに到達し、最終的に大量のスパムがメール・ストアに入り込むこととなります。しかし、Cloudmark ActiveFilter を導入すれば、既存の防御システムを通り抜けたスパムを削除し、フィルタリング精度を 99% を超えるレベルに高めることができます。

Cloudmark の特長

Cloudmark のソリューションは、最初のスキャンで見逃されて受信トレイに入ってしまったわずかなスパム・メッセージも数秒後に特定し、受信者が受信トレイを表示する前にこの作業を何度も繰り返し実行します。Cloudmark ActiveFilter for Mail Stores では、新しいフィンガープリントを継続的にチェックし、メール・ストアに配信されたメッセージがスパムかどうかを確認するという手法を採用し、スパムの捕捉率と捕捉精度の向上を図っています。この手法により、強力な IP 評価機能、スロットリング機能、コンテンツ・フィルタリング機能をもとめせずに侵入したスパム・メッセージに対し、過去に遡って対応することが可能になるため、スパム・フィルタの更新で生じる遅延を利用しようとする高速な攻撃の影響を大幅に低減することができます。

見逃されてしまったスパム・メッセージを検出するために一般的なキャリアがメール・ストア全体を再スキャンすることは現実的ではありません。メール・ストアに格納された数テラバイトから数ペタバイトのデータの再処理には大量のリソースが必要になるからです。Cloudmark ActiveFilter では、メール・ストア内の物理的なメッセージを再スキャンする必要がありません。代わりに、最初に配信された際にスパムとして識別し格納した特定のメッセージのみを移動または削除する「プッシュ」パラダイムを利用し、CPU への影響を最小限に抑えることができます。

迅速かつ効率的なスパム対策

Cloudmark のソリューションは、Advanced Message Fingerprinting™ テクノロジーと、Cloudmark Global Threat Network (190 カ国にまたがる 8 億 5,000 万人もの信頼できるユーザが参加) からリアルタイムにレポートされるスパム情報を独自の方法で連携させ、迅速かつ効率的なスパム対策を実現します。最初に、Advanced Message Fingerprinting が 1 つのスパム・メッセージを一組の軽量のフィンガープリントに変換してスキャンします。そのあとは、Cloudmark ActiveFilter が、スキャン後にメール・ストアに送られたフィンガープリントをキャッシュしながら、最新のフィンガープリントが Global Threat Network から届いているかどうかを継続的に監視します。新たに特定されたスパム・フィンガープリントと一致するメッセージがメール・ストア内にあることが判明した場合には、そのメッセージに対してのみ処理を実行するように Cloudmark ActiveFilter がメール・ストアに指示します。

また、Cloudmark ActiveFilter は、従来のコンテンツ・フィルタを回避できるように設計された高度なスパム配信技術の強みをほぼ無効にして、メール・ストア内のスパム・レベルを大幅に低減し、CPU およびディスク・リソースへの影響を最小限に抑えます。

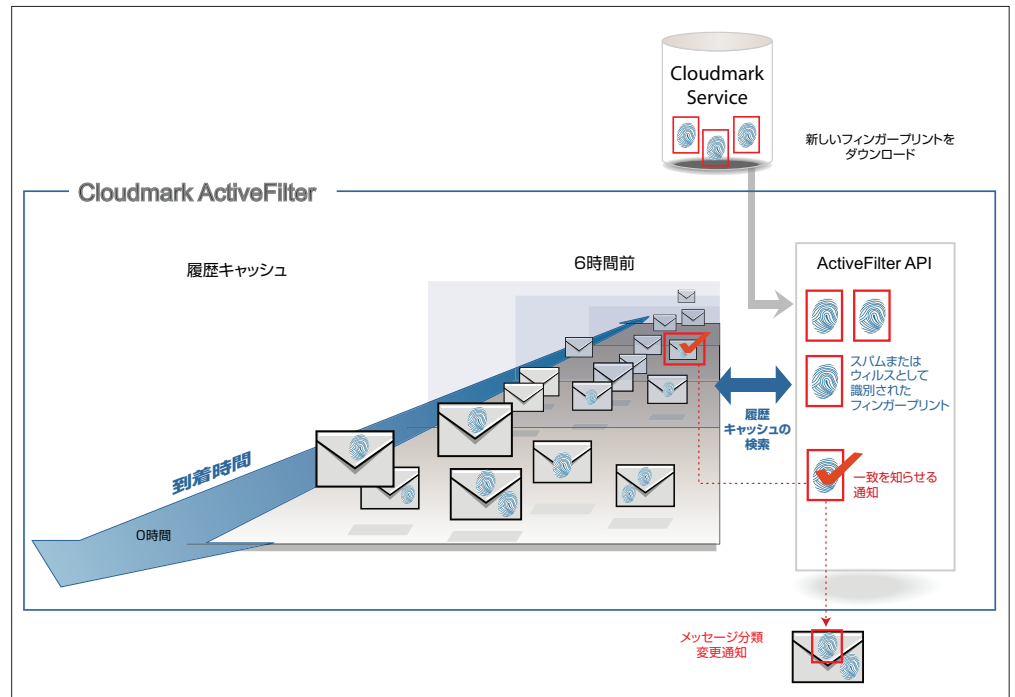
Cloudmark について

キャリアグレード・メッセージング・セキュリティのグローバル・リーダーである Cloudmark は、精度、包括性、性能で業界をリードするスパム、ウィルス、フィッシング対策ソリューションを提供しています。モバイル・ネットワーク、固定ネットワーク、ソーシャル・ネットワークに対応する Cloudmark 独自のソリューションは、Advanced Message Fingerprinting と、Global Threat Network (190 カ国にまたがる 8 億 5,000 万人の信頼できるレポートが参加) からリアルタイムに送られてくるフィードバック情報を連携させ、メッセージング・インフラのあらゆるポイントで高度なフィルタリングおよびセキュリティを実現します。なお、現時点で 8 億 5,000 万以上のメールボックスを保護している Cloudmark ソリューションは、世界中のモバイル・オペレータやホスティング・プロバイダを含め、100 社以上のサービス・プロバイダに導入されています。

Cloudmark ActiveFilter のプロセス・フロー

Cloudmark ActiveFilter は、最初の受信時にゲートウェイ MTA によってスキャンされ問題が検出されなかったメッセージのフィンガープリントも追跡し、キャッシュに格納します。のちに、Cloudmark Authority が新しいスパム・フィンガープリントを発見しダウンロードすると、このフィンガープリントをキャッシュ内のフィンガープリントと比較し、最初に問題が検出されなかったメッセージが、見逃されたスパムでなかったかを確認します。

ActiveFilter は、見逃されたスパム・メッセージを検出した際に、ユーザのポリシーで規定されている措置に従って、このメッセージをバックエンドのメール・ストア・ホスト上で修正する機能も搭載しています。この機能により、スパム・メッセージの削除やユーザのジャンク・フォルダへの移動も可能となっています。



詳細は www.cloudmark.com をご覧ください。

日本事業所
クラウドマーク ジャパン
〒107-0052
東京都港区赤坂 4-13-5
赤坂オフィスハイツ 131
電話: 03-6277-8816
Fax: 03-6277-8829
電子メール: japan@cloudmark.com

北米事業所
Cloudmark, Inc. (本社)
128 King Street, 2nd Floor
San Francisco, CA 94107 USA
電話: +1-415-543-1220
Fax: +1-415-543-1233